

## IT Applications Unit 4 Self-test Chapter 8

### Multiple Choice

Identify the choice that best completes the statement or answers the question.

- ☐ 1. The use of physical human characteristics or behavioural characteristics to grant access to data is known as:
- a. physical security.
  - b. biometrics.
  - c. bionics.
  - d. hardware security.
- ☐ 2. The most accurate biometric system available is believed to be:
- a. hand geometry.
  - b. signature verification.
  - c. iris recognition.
  - d. fingerprint recognition.
- ☐ 3. A card used for security purposes that contains a microchip that can store data is called a:
- a. swipe card.
  - b. smart card.
  - c. intelligent card.
  - d. security token.
- ☐ 4. A device used to protect against power fluctuations and supply power in the case of power loss is known as a/an:
- a. uninterruptible power supply.
  - b. surge protector.
  - c. spike protector.
  - d. universal power system.
- ☐ 5. A system that continues to work due to redundancies built into the system, even when a piece of hardware has failed, is known as a/an:
- a. online system.
  - b. backup system.
  - c. fault-tolerant system.
  - d. security system.
- ☐ 6. A method of guarding against hard disk failure where fragments of data are spread over several hard drives is known as a:
- a. RAID.
  - b. disk mirroring system.
  - c. mirror server.
  - d. hard drive backup.
- ☐ 7. Magnetic media used for backup include:
- a. online backup.

- b. CDs and DVDs.
- c. USB storage devices.
- d. hard disk drives.

☐

8. One of the main differences between magnetic tape and other forms of backup media is:

- a. data is accessed sequentially on a magnetic tape, not randomly.
- b. magnetic tapes can hold a smaller amount of data than most other media.
- c. tape drives cannot be built into computer systems and must be connected externally.
- d. magnetic tapes provide a much faster form of backing up files.

☐

9. Diagnostic tools that monitor the contents of packets being sent across data networks are known as:

- a. filter packets.
- b. packet sniffers.
- c. desktop monitoring tools.
- d. audit trails.

☐

10. Log files of system logins and records of files accessed, modified or copied are known as:

- a. audit trails.
- b. desktop monitoring programs.
- c. packet sniffers.
- d. window log files.

☐

11. Physical security devices include:

- a. audit trails and log files.
- b. hard disk drives and magnetic tapes
- c. encryption and anti-virus software.
- d. lockable boxes and security cables.

☐

12. An ideal password should be:

- a. something that is easy to guess or decipher.
- b. the name of a partner or favourite pet.
- c. a combination of letters and digits at least six characters in length.
- d. kept the same on a long-term basis.

☐

13. Firewalls are used to:

- a. protect from all types of viruses.
- b. restrict unauthorised access to a network.
- c. monitor employee access to data.
- d. convert electronic data to an unreadable, coded format.

☐

14. Each document should have which of the following included in the filename?

- a. Information about when the document was created and last saved
- b. Information about the folder location and network
- c. Information about timeliness of the document and file version
- d. Which users can access the file for updating purposes

- ☐ 15. A differential backup:
- a. is another name for a full backup.
  - b. only copies files that have been created since the last full backup.
  - c. only copies files that have been changed since the last partial backup.
  - d. only copies files that have been changed since the last full backup.
- ☐ 16. The safest strategy for storage of backup media for an organisation would be:
- a. one copy kept onsite in a fireproof lockable cabinet.
  - b. one copy kept in a secure location offsite.
  - c. two copies – one kept onsite in the server room, one kept in a secure location offsite.
  - d. two copies – one kept onsite in a fireproof, lockable cabinet, one kept in a secure location offsite.
- ☐ 17. The process of copying files to long-term storage and removing them from the hard disk is known as:
- a. archiving.
  - b. backup.
  - c. destruction.
  - d. deletion.
- ☐ 18. An advantage for businesses that utilise cloud computing is:
- a. not having to invest large amounts of money in optical devices.
  - b. not having to invest large amounts of money in ISP costs.
  - c. not having to invest large amounts of money in infrastructure and software.
  - d. not having to invest large amounts of money in toner cartridges.
- ☐ 19. The part of a disaster recovery plan that includes specific procedures for restoring the full processing capacity of an organisation is called:
- a. an emergency plan.
  - b. a backup plan.
  - c. a recovery plan.
  - d. a test plan.
- ☐ 20. A data security strategy could be said to be effective if:
- a. users frequently need assistance with forgotten passwords.
  - b. data can be accessed and restored when required.
  - c. files cannot be easily located.
  - d. data can be accessed by all workers and outsiders.